#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Identity Alliance (IDA)	Tim Jurgensen (TMJ)	TE	1	63	1	The Framework adopts a much too restrictive definition for "privacy". It essentially equates "privacy" with "secrecy". In fact, privacy equates to decisional control over all aspects of a person's involvement in an interaction and in ownership of the consequences of that interaction. It is by assertions of personal privacy that a person engages interactions through which reputation is established. Reputation is central to the level of trust implicit in a person's involvement in interactions going forward. The tendency within this iteration of the Framework is to view privacy as something that can be forfeited as a means of risk amelioration. In fact, the personal privacy of the end users of all systems must be an ongoing consideration in risk assessment.	Rethink the document to more substantially include the end user within the considered infrastructure as opposed to the current undue emphasis only on service providers. This extension is necessary in order to properly assess the value to be associated with risks. For the service provider, it may be acceptable to sever access of the end user to "protect" the infrastructure. For the end user, losing access may incure debilitating harm. A proper risk assessment must weigh the potential risk mitigation for the service provider with the potentially unwarranted risk of real damage done to the end user. Essentially, the requirement is for a balanced assessment of technical capability and social policy versus personal privacy. As an initial aspect of every interaction, the personal privacy decisions of the service provider and the end-user must be established through a conditional covenant (a contract). Constraints on this covenant may be imposed by the governing policy infrastructure.

2	IDA	TMJ	TE	1	64	1	The concept of "risk" as used throughout this document is strongly oriented toward the service provider end of the spectrum and is therefore quite pejorative toward the personal privacy of end users. The concept of "trust", which has a reciprocal relationship to "risk" might be a preferable approach to achieve a more balanced perspective. A "Cybersecurity Framework" is much more reasonably understood as a "trust infrastructure" than as a "risk infrastructure".	Rethink the document to consider whether presentation of the Framework as a "trust infrastructure" might offer a more compelling "social protcol" environment. It seems easier to understand the propagation of trust through well defined processes than to understand the propagation of "risk amelioration" in a similar vein. In particular, if one is concerned only with risk, it is easy to forget about the value of services to the end-user. The loss of potential business to the service provider does not equate with the loss of opportunity to the end user that derives from the services; both perspectives must be considered in risk assessment.
3	IDA	TMJ	TE	1	67	1	The concept of "voluntary" is somewhat ambiguous. It would be useful to expand on just what this means.	Consider "voluntary" from the perspective of public roadways. Each person (service provider) can "voluntarily" make use of the roadway. However, if they choose to do so then the person and their vehicle comes under the purview of standards (rules, regulations and enforcement mechanisms) established by a superior governing entity (policy infrastructure) for the "public system".
4	IDA	TMJ	TE	1	71	1	Critical infrastructure is defined as encompassing both physical and virtual elements. Consequently, it should be only a matter of both physical capability as well as policy selection whether a "voluntary" entity enters the Framework.	Make clear that non-participants (non-volunteers) can be physically excluded from the Framework. This requirement will prevent non-volunteers from gaining undue benefit by appearing in coexistence with true, functioning participants of the Framework.
5	IDA	TMJ	TE	1	88	1	Reference to best practices "to achieve outcomes…" is better understood within the concept of a trust infrastructure.	This point would seem to reinforce the suggestion in Comment 2.
6	IDA	TMJ	TE	1	99	1	Note the reference to "internal" and "external" stakeholders.	This point would seem to reinforce the suggestion in Comment 1.

7	IDA	TMJ	TE	2	119	1.1	The five functions of the Framework Core are not at quivalent semantic levels.	There are actually four core functions of "Protect, Detect, Respond, Recover" that can be viewed as characteristics of "homeostatic regulation". This property of living organisms seems applicable to technical systems as well. However, it is useful to view these functions as being achieved through a collection of subordinate facilities: Opacity, Integrity, Identity, Authority, Attribution. Each of these facilities can make use of a variety of technical processes in order to achieve the main (four) core functions. This approach allows a better decomposition of the core functions into processes that are common across the functions. The concept of "Identify" should be viewed either as superior or inferior to the other core functions, but not the semantic equivalent.
8	IDA	TMJ	TE	2	140	1.1	The Framework encompasses social as well as technical perspectives. Industry standards and best practices will encompass social as well as technical processes.	Consider reference to "Framework Protocols" as the means for realizing "Framework Profiles".
9	IDA	TMJ	TE	5	207	2.1	The Framework Core must encompass social processes as well as technical processes. Consequently, the decomposition of the main functions must reference legal (social) constraints as well as technical constraints.	Viewing the Framework as purely a voluntary, technical domain ignores issues that propagate into the social domain. For example, for an end-user to recover from identity theft requires the Framework and its processes to seamlessly meld with legal processes. This impacts the relevant standards and best practices applicable to realize the core functions.

10	IDA	TMJ	TE	6	243	2.1	The concept of "Identify" as presented here is dependent on developing an "experiential memory" of complex processes. This requires a more complete understanding of the subprocesses on which the core functions are based.	Consider recognizing a set of primitive processes and delving into their definitions in more detail. In Comment 7 a set of primitives was listed: Opacity, Integrity, Identity, Authority, Attribution. An equivalent but orthogonal list might be developed. The important point is to be able to decompose the core functions into primitive processes that can readily cross the boundaries between functions.
11	IDA	TMJ	TE	6	252	2.1	To "Protect" suggests prioritization through an organization's risk management process. This should be expanded to encompass the risk management process of the end user and of the encompassing policy infrastructure within which the organization exists.	Expand the prioritization process to include both the encompassing policy infrastructure as well as the end-user community.
12	IDA	TMJ	TE	7	259	2.1	Apply Comment 11 rationale to "Detect".	Apply Comment 11 suggestion to "Detect".
13	IDA	TMJ	TE	7	265	2.1	Apply Comment 11 rationale to "Respond".	Apply Comment 11 suggestion to "Respond".
14	IDA	TMJ	TE	7	273	2.1	Apply Comment 11 rationale to "Recover".	Apply Comment 11 suggestion to "Recover".
15	IDA	TMJ	TE	7	281	2.2	A "Framework Profile" seems a reasonable way to define a target. However, it implies a more static state.	Consider defining "Framework Protocols" as the means to achieve specific profile states. This will require the description of dynamic processes coupled to more static state variables.
16	IDA	TMJ	TE	9	321	2.4	The Framework Implementation Tiers appears restricted within the confines of a service provider organization. This would not appear to adequately address the concerns of the potential users of those services.	Exand the risk management perspective to encompass the end user community within the mandates of the encompassing policy infrastructure. This will likely change the results of the risk assessment and management process.
17	IDA	TMJ	TE	12	450	3.4	As has been noted in previous comments, the current Framework specification does not appear to adequately encompass the end user communities of infrastructure services, nor the policy mandates of the encompassing policy infrastructure.	Expand the applicable reference material to include the social (policy) environment that encompasses the relevant infrastructure, service providers and end users of all services.
